McAfee Labs Threat Advisory

Ransomware-Petya

April 11, 2016

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive “Malware and Threat Reports” at the following URL**:** https://sns.snssecure.mcafee.com/content/signup_login.

Summary

Ransomware-Petya is different than regular ransomware in that upon execution, it infects low-level structure (MBR [Master Boot Record], MFT [Master File Table]) and doesn’t allow the computer to boot normally. It will infect MBR and on restart, it has its own low language code to encrypt MFT, which makes the drive inaccessible.

This threat is detected under the following detection name:

- Ransom-Petya

Detailed information about the threat, its propagation, characteristics, and mitigation are in the following sections:

Infection and Propagation Vectors

This malware is known to be propagated via spam emails that contain a link to a dropbox shared .zip file. This archive contains a .jpg photo and the actual malware executable. Known filenames of the photo and executable:

- Bewerbungsbild.jpg
- Bewerbungsfoto.jpg
- Bewerbungspoto.jpg
- Bewerbungsmappe-gepackt.exe
- Bewerbungsunterlagen.PDF.exe
- BewerbungsmappePDF.exe

Mitigation

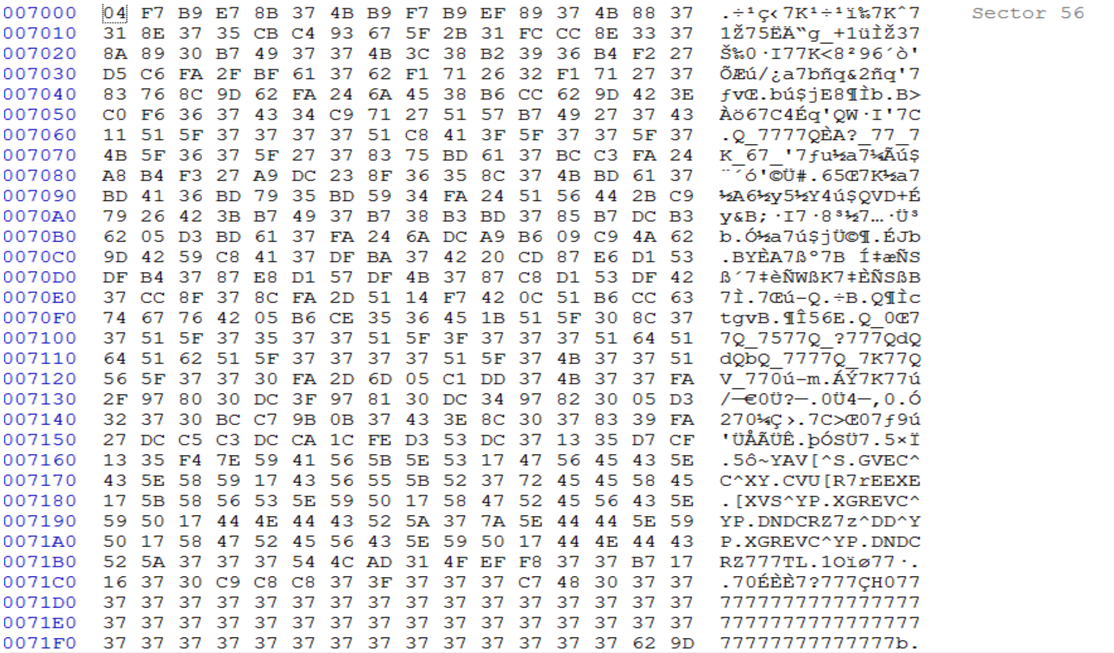
The basic mitigation methods for such infection are the usual best practices in network security. By following them and training users to follow them, the chance of getting infected by ransomware is lowered considerably:

- Avoid opening attachments in emails from untrusted sources. If your company allows, implement rules to block attachments with common executable extensions.
- Avoid opening links in email and chat windows from untrusted sources, and double-check them if they are sent by a trusted connection. Sometimes an infected machine may send links to all contacts found in the email/chat application, which would appear to the destination as if coming from a trusted contact.
- Keep all of your software up to date, including your operating system, Office package, browser, and any plugins you may be using. Disable any unnecessary plugins to avoid the extra attack surface.
- Keep your Antivirus up to date to help avoid other infections that may bring the ransomware to your machine.

Characteristics and Symptoms

Description

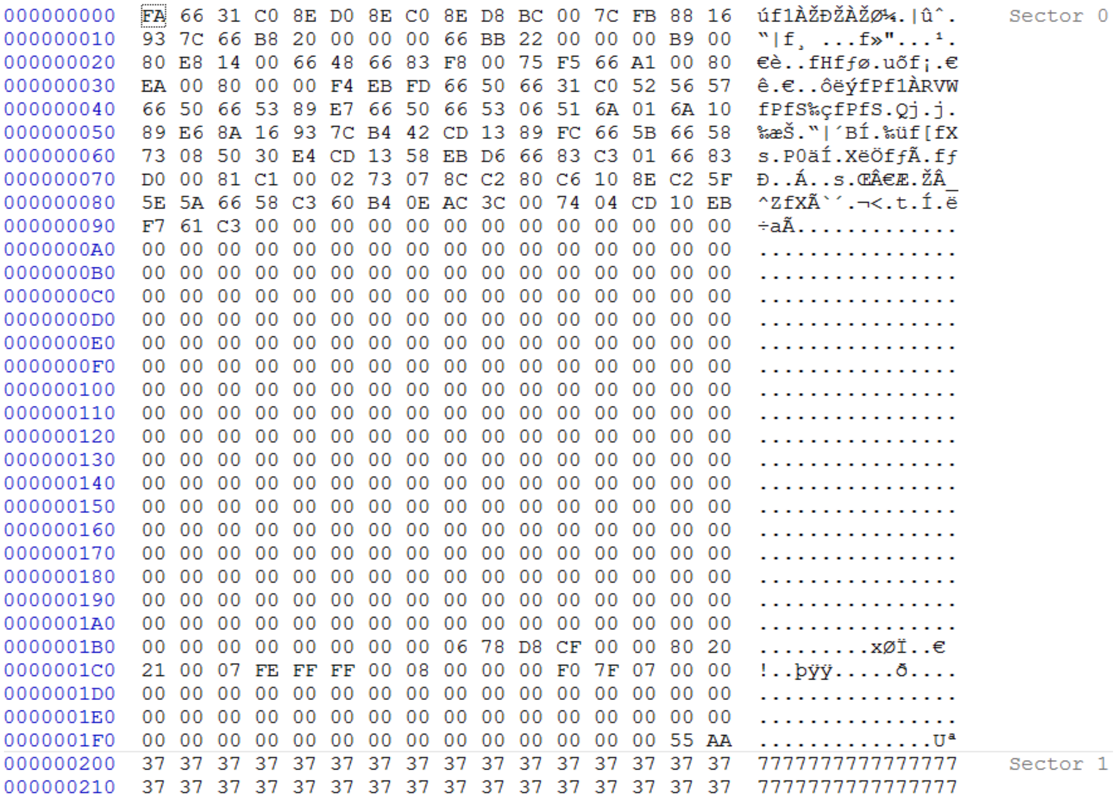
Upon execution, Ransomware-Petya will show the UAC window to gain the Administrator privilege to execute the binary. After it runs, it will keep original MBR with simple byte-wise XOR operation to sector 56 (XoR Key = 0x37).



```
007000  04 F7 B9 E7 8B 37 4B B9 F7 B9 EF 89 37 4B 88 37  .÷¹ç‹7K¹÷¹ï‰7Kˆ7    Sector 56
007010  31 8E 37 35 CB C4 93 67 5F 2B 31 FC CC 8E 33 37  1Ž75ËÄ“g_+1üÌŽ37
007020  8A 89 30 B7 49 37 37 4B 3C 38 B2 39 36 B4 F2 27  Š‰0·I77K<8²96´ò'
007030  D5 C6 FA 2F BF 61 37 62 F1 71 26 32 F1 71 27 37  ÕÆú/¿a7bñq&2ñq'7
007040  83 76 8C 9D 62 FA 24 6A 45 38 B6 CC 62 9D 42 3E  ƒvŒ.bú$jE8¶Ìb.B>
007050  C0 F6 36 37 43 34 C9 71 27 51 57 B7 49 27 37 43  Àö67C4Éq'QW·I'7C
007060  11 51 5F 37 37 37 37 51 C8 41 3F 5F 37 37 5F 37  .Q_7777QÈA?_77_7
007070  4B 5F 36 37 5F 27 37 83 75 BD 61 37 BC C3 FA 24  K_67_'7ƒu½a7¼Ãú$
007080  A8 B4 F3 27 A9 DC 23 8F 36 35 8C 37 4B BD 61 37  ¨´ó'©Ü#.65Œ7K½a7
007090  BD 41 36 BD 79 35 BD 59 34 FA 24 51 56 44 2B C9  ½A6½y5½Y4ú$QVD+É
0070A0  79 26 42 3B B7 49 37 B7 38 B3 BD 37 85 B7 DC B3  y&B;·I7·8³½7…·Ü³
0070B0  62 05 D3 BD 61 37 FA 24 6A DC A9 B6 09 C9 4A 62  b.Ó½a7ú$jÜ©¶.ÉJb
0070C0  9D 42 59 C8 41 37 DF BA 37 42 20 CD 87 E6 D1 53  .BYÈA7ß°7B Í‡æÑS
0070D0  DF B4 37 87 E8 D1 57 DF 4B 37 87 C8 D1 53 DF 42  ß´7‡èÑWßK7‡ÈÑSßB
0070E0  37 CC 8F 37 8C FA 2D 51 14 F7 42 0C 51 B6 CC 63  7Ì.7Œú-Q.÷B.Q¶Ìc
0070F0  74 67 76 42 05 B6 CE 35 36 45 1B 51 5F 30 8C 37  tgvB.¶Î56E.Q_0Œ7
007100  37 51 5F 37 35 37 37 51 5F 3F 37 37 37 51 64 51  7Q_7577Q_?777QdQ
007110  64 51 62 51 5F 37 37 37 37 51 5F 37 4B 37 37 51  dQbQ_7777Q_7K77Q
007120  56 5F 37 37 30 FA 2D 6D 05 C1 DD 37 4B 37 37 FA  V_770ú-m.ÁÝ7K77ú
007130  2F 97 80 30 DC 3F 97 81 30 DC 34 97 82 30 05 D3  /—€0Ü?—.0Ü4—‚0.Ó
007140  32 37 30 BC C7 9B 0B 37 43 3E 8C 30 37 83 39 FA  270¼Ç›.7C>Œ07ƒ9ú
007150  27 DC C5 C3 DC CA 1C FE D3 53 DC 37 13 35 D7 CF  'ÜÅÃÜÊ.þÓSÜ7.5×Ï
007160  13 35 F4 7E 59 41 56 5B 5E 53 17 47 56 45 43 5E  .5ô~YAV[^S.GVEC^
007170  43 5E 58 59 17 43 56 55 5B 52 37 72 45 45 58 45  C^XY.CVU[R7rEEXE
007180  17 5B 58 56 53 5E 59 50 17 58 47 52 45 56 43 5E  .[XVS^YP.XGREVC^
007190  59 50 17 44 4E 44 43 52 5A 37 7A 5E 44 44 5E 59  YP.DNDCRZ7z^DD^Y
0071A0  50 17 58 47 52 45 56 43 5E 59 50 17 44 4E 44 43  P.XGREVC^YP.DNDC
0071B0  52 5A 37 37 37 54 4C AD 31 4F EF F8 37 37 B7 17  RZ777TL.1Oïø77·.
0071C0  16 37 30 C9 C8 C8 37 3F 37 37 37 C7 48 30 37 37  .70ÉÈÈ7?777ÇH077
0071D0  37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37  7777777777777777
0071E0  37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37  7777777777777777
0071F0  37 37 37 37 37 37 37 37 37 37 37 37 37 37 62 9D  77777777777777b.
```

XOR with 0x37

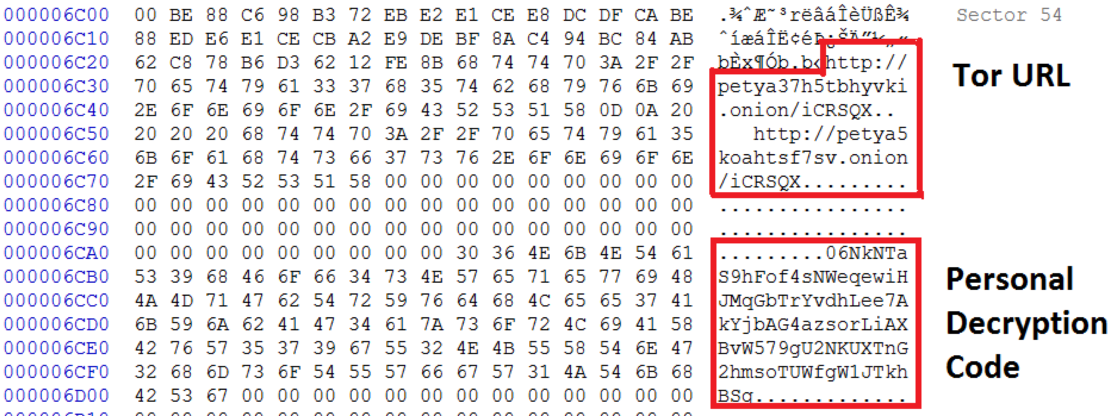
Later, it will overwrite MBR with its own code. It also fills its own content for the next 32 sectors and will perform simple byte-wise XOR encryption to next 32 sectors (with same XoR key 0x37).



```
000000000  FA 66 31 C0 8E D0 8E C0 8E D8 BC 00 7C FB 88 16  úf1ÀŽÐŽÀŽØ¼.|ûˆ.    Sector 0
000000010  93 7C 66 B8 20 00 00 00 66 BB 22 00 00 00 B9 00  “|f¸ ...f»"...¹.
000000020  80 E8 14 00 66 48 66 83 F8 00 75 F5 66 A1 00 80  €è..fHfƒø.uõf¡.€
000000030  EA 00 80 00 00 F4 EB FD 66 50 66 31 C0 52 56 57  ê.€..ôëýfPf1ÀRVW
000000040  66 50 66 53 89 E7 66 50 66 53 06 51 6A 01 6A 10  fPfS‰çfPfS.Qj.j.
000000050  89 E6 8A 16 93 7C B4 42 CD 13 89 FC 66 5B 66 58  ‰æŠ.“|´BÍ.‰üf[fX
000000060  73 08 50 30 E4 CD 13 58 EB D6 66 83 C3 01 66 83  s.P0äÍ.XëÖfƒÃ.fƒ
000000070  D0 00 81 C1 00 02 73 07 8C C2 80 C6 10 8E C2 5F  Ð..Á..s.ŒÂ€Æ.ŽÂ_
000000080  5E 5A 66 58 C3 60 B4 0E AC 3C 00 74 04 CD 10 EB  ^ZfXÃ`´.¬<.t.Í.ë
000000090  F7 61 C3 00 00 00 00 00 00 00 00 00 00 00 00 00  ÷aÃ.............
0000000A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000000B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000000C0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000000D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000000E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000000F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000110  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000120  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000130  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000140  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000150  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000160  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000170  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000180  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000000190  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000001A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000001B0  00 00 00 00 00 00 00 00 06 78 D8 CF 00 00 80 20  .........xØÏ..€ 
0000001C0  21 00 07 FE FF FF 00 08 00 00 00 F0 7F 07 00 00  !..þÿÿ.....ð....
0000001D0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000001E0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0000001F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 55 AA  ..............Uª
000000200  37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37  7777777777777777    Sector 1
000000210  37 37 37 37 37 37 37 37 37 37 37 37 37 37 37 37  7777777777777777
```

Overwritten MBR & XOR sector 1 with 0x37

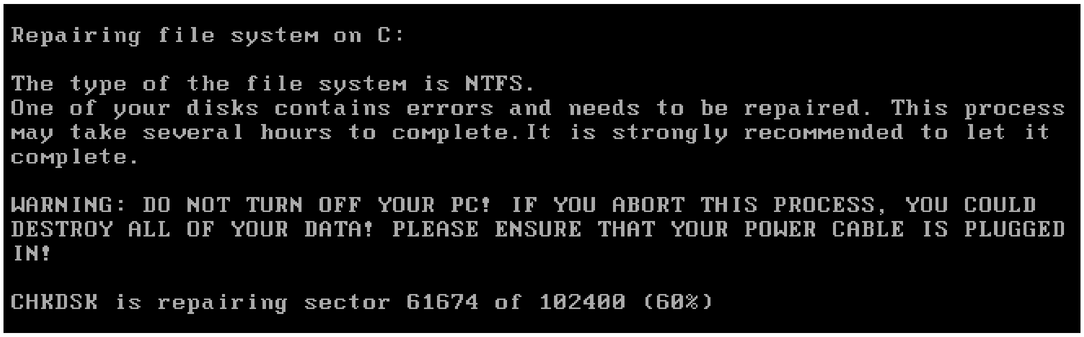
Malware keeps its 16-bit code from sector 34 to 49, which has booting image and encryption and decryption routines.
In Sector 54, it will write a personal decryption code and TOR URL.



```
000006C00  00 BE 88 C6 98 B3 72 EB E2 E1 CE E8 DC DF CA BE  .¾ˆÆ˜³rëâáÎèÜßÊ¾   Sector 54
000006C10  88 ED E6 E1 CE CB A2 E9 DE BF 8A C4 94 BC 84 AB  ˆíæáÎË¢éÞ¿ŠÄ”¼„«
000006C20  62 C8 78 B6 D3 62 12 FE 8B 68 74 74 70 3A 2F 2F  bÈx¶Ób.b‹http://
000006C30  70 65 74 79 61 33 37 68 35 74 62 68 79 76 6B 69  petya37h5tbhyvki
000006C40  2E 6F 6E 69 6F 6E 2F 69 43 52 53 51 58 0D 0A 20  .onion/iCRSQX..
000006C50  20 20 20 68 74 74 70 3A 2F 2F 70 65 74 79 61 35     http://petya5
000006C60  6B 6F 61 68 74 73 66 37 73 76 2E 6F 6E 69 6F 6E  koahtsf7sv.onion
000006C70  2F 69 43 52 53 51 58 00 00 00 00 00 00 00 00 00  /iCRSQX.........
000006C80  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000006C90  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
000006CA0  00 00 00 00 00 00 00 00 00 30 36 4E 6B 4E 54 61  .........06NkNTa
000006CB0  53 39 68 46 6F 66 34 73 4E 57 65 71 65 77 69 48  S9hFof4sNWeqewiH
000006CC0  4A 4D 71 47 62 54 72 59 76 64 68 4C 65 65 37 41  JMqGbTrYvdhLee7A
000006CD0  6B 59 6A 62 41 47 34 61 7A 73 6F 72 4C 69 41 58  kYjbAG4azsorLiAX
000006CE0  42 76 57 35 37 39 67 55 32 4E 4B 55 58 54 6E 47  BvW579gU2NKUXTnG
000006CF0  32 68 6D 73 6F 54 55 57 66 67 57 31 4A 54 6B 68  2hmsoTUWfgW1JTkh
000006D00  42 53 67 00 00 00 00 00 00 00 00 00 00 00 00 00  BSg.............
```

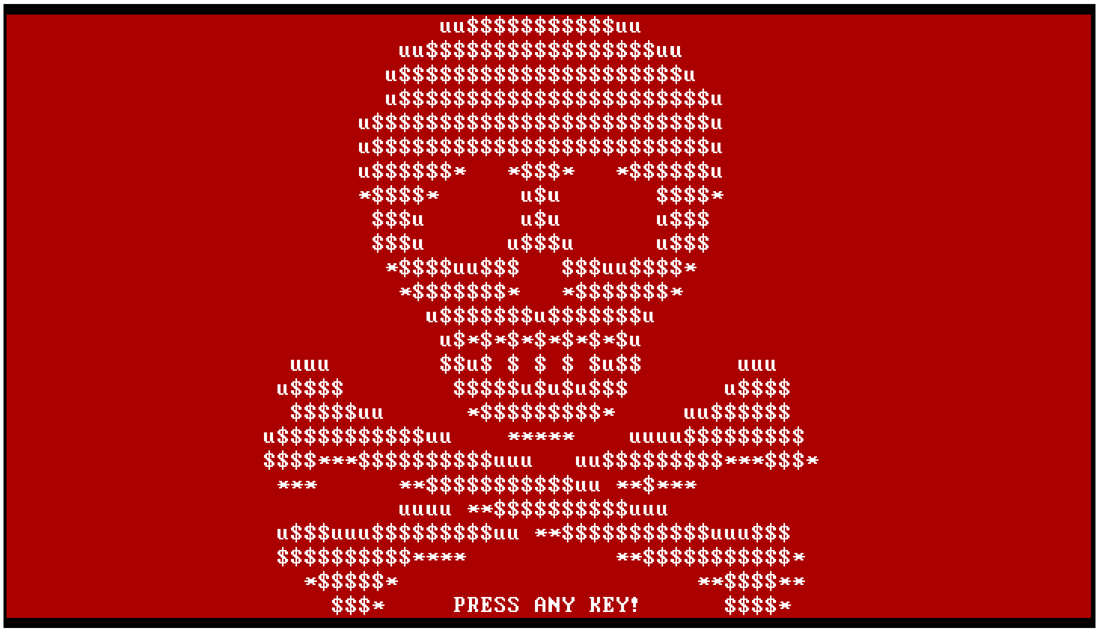
It will then adjust privilege to SeShutDownPrivilege, and use the undocumented Windows API “**NtRaiseHardError”** to create a blue screen to restart the infected system.

On reboot, it will show the following screen showing “chkdsk” is repairing. While showing this, it will encrypt the **Master File Table.(MFT)**:



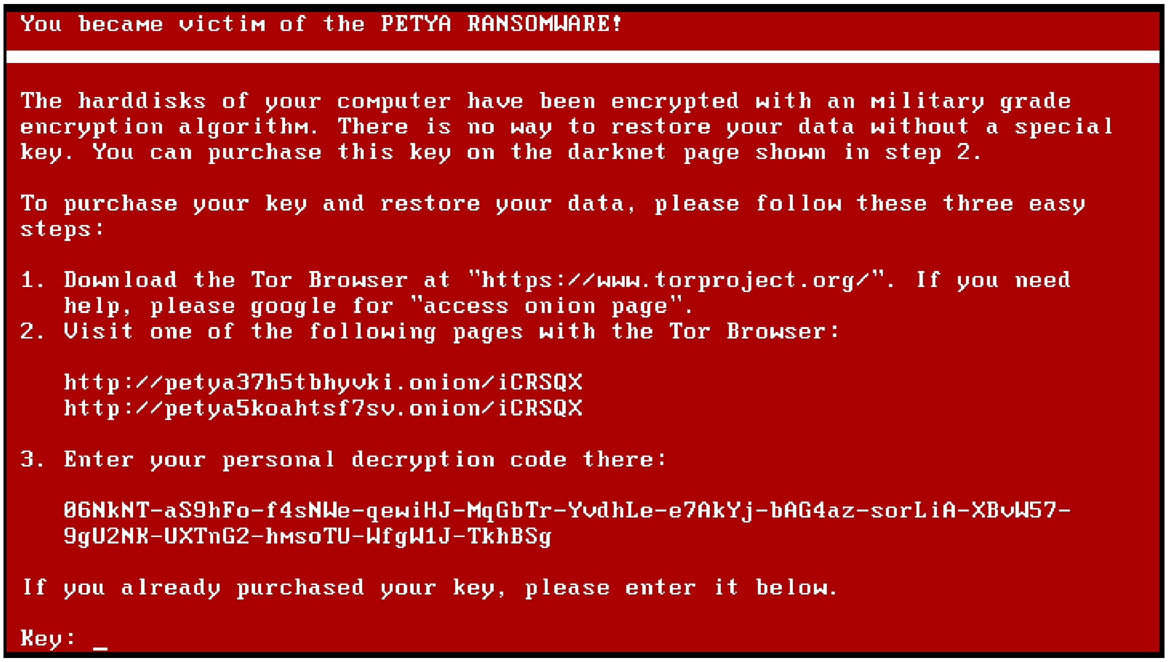
```
Repairing file system on C:

The type of the file system is NTFS.
One of your disks contains errors and needs to be repaired. This process
may take several hours to complete.It is strongly recommended to let it
complete.

WARNING: DO NOT TURN OFF YOUR PC! IF YOU ABORT THIS PROCESS, YOU COULD
DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED
IN!

CHKDSK is repairing sector 61674 of 102400 (60%)
```

After it encrypts MFT, it will show the red skeleton screen (Danger):



```
             uu$$$$$$$$$$$uu
          uu$$$$$$$$$$$$$$$$$uu
         u$$$$$$$$$$$$$$$$$$$$$u
         u$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$$$$$$$$$$$$$$$$$$$$u
       u$$$$$$*   *$$$*   *$$$$$$u
       *$$$$*      u$u       $$$$*
        $$$u       u$u       u$$$
        $$$u      u$$$u      u$$$
         *$$$$uu$$$   $$$uu$$$$*
          *$$$$$$$*   *$$$$$$$*
            u$$$$$$$u$$$$$$$u
             u$*$*$*$*$*$*$u
  uuu        $$u$ $ $ $ $u$$       uuu
 u$$$$        $$$$$u$u$u$$$       u$$$$
  $$$$$uu      *$$$$$$$$$*     uu$$$$$$
u$$$$$$$$$$$uu    *****    uuuu$$$$$$$$$
$$$$***$$$$$$$$$$uuu   uu$$$$$$$$$***$$$*
 ***      **$$$$$$$$$$$uu **$***
          uuuu **$$$$$$$$$$uuu
 u$$$uuu$$$$$$$$$uu **$$$$$$$$$$$uuu$$$
 $$$$$$$$$$****           **$$$$$$$$$$$*
   *$$$$$*                      **$$$$**
     $$$*     PRESS ANY KEY!      $$$$*
```

Finally, it will show TOR URLs asking for ransom for the victim machine. At this stage the malware has encrypted MFT, which makes the disk unreadable even if you access the disk from other devices.



```
You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade
encryption algorithm. There is no way to restore your data without a special
key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy
steps:

1. Download the Tor Browser at "https://www.torproject.org/". If you need
   help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

   http://petya37h5tbhyvki.onion/iCRSQX
   http://petya5koahtsf7sv.onion/iCRSQX

3. Enter your personal decryption code there:

   06NkNT-aS9hFo-f4sNWe-qewiHJ-MqGbTr-YvdhLe-e7AkYj-bAG4az-sorLiA-XBvW57-
   9gU2NK-UXTnG2-hmsoTU-WfgW1J-TkhBSg

If you already purchased your key, please enter it below.

Key: _
```

Restart Mechanism

As explained above, Ransomware-Petya will modify the original MBR (Clean) with its malicious MBR. On reboot, a malicious MBR will load and perform the malicious activities.

Indicators of Compromise (IOC)

User will not be able to boot the infected system, and the above mentioned screenshots will be displayed during boot time.

This Threat Advisory is for the education and convenience of Intel Security customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.